REMARKS

[0003] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. Claims 1-3, 6-10, and 13-43 are presently pending. Claim 1 is amended herein. Claims 4, 5, 11, and 12 are cancelled herein. New claims 41-43 are added herein.

Statement of Substance of Interview

[0004] The Examiner graciously spoke with me—the undersigned representative for the Applicant—on November 21, 2008, by phone. Applicant greatly appreciates the Examiner's willingness to talk. Such willingness is invaluable to both of us in our common goal of an expedited prosecution of this patent application.

[0005] During the interview, we discussed how the claims differed from the cited references, particularly differences between the claimed "correctness detection action" and the cited *conformance test* of Elgamal. Without conceding the propriety of the rejections and in the interest of expediting prosecution, I also proposed several possible clarifying amendments.

[0006] I understood the Examiner to tentatively concur with assessment of Elgamal and the proposed amendment to independent claim 1, subject to reconsidering the claims and the references upon submission of the formal response herein.

[0007] Applicant herein amends the claims consistent with the discussion during the interview. Accordingly, Applicant submits that the pending claims are allowable over the cited art of record for at least the reasons discussed during the interview.

Formal Request for an Interview

[0008] If the Examiner's reply to this communication is anything other than allowance of all pending claims, then I formally request an interview with the Examiner. I encourage the Examiner to call me—the undersigned representative for the Applicant—so that we can talk about this matter so as to resolve any outstanding issues quickly and efficiently over the phone.

[0009] Please contact me to schedule a date and time for a telephone interview that is most convenient for both of us. While email works great for me, I welcome your call as well. My contact information may be found on the last page of this response.

Claim Amendments and Additions

[0010] Without conceding the propriety of the rejections herein and in the interest of expediting prosecution, Applicant amends claim 1 herein. Applicant amends the claim to highlight claimed features. Such amendments are made to expedite prosecution and more quickly identify allowable subject matter. The amendment should not be construed as further limiting the claimed invention in response to the cited references.

[0011] Claim 1 is amended to include subject matter from canceled dependent claims. Furthermore, Applicant adds new claims 41-43 herein. These new claims are fully supported by application as originally filed and therefore do not constitute new matter. These new claims are allowable over the cited references at least due to their dependence from a base claim which Applicant submits is allowable over the cited references for at least the reasons discussed herein.

Substantive Matters

Claim Rejections under § 103

[0012] Claims 1-40 are rejected under 35 U.S.C. § 103. Applicant respectfully traverses the rejection of these claims. In light of the remarks and amendments presented herein and the discussion during the above-discussed Examiner interview, Applicant asks the Examiner to withdraw these rejections.

[0013] The Examiner's rejections are based upon the following references in combination:

- **Elgamal:** *Elgamal, et al.,* US Patent No. 6,397,330 (issued May 28, 2002);
- **De Bonet:** *De Bonet, et al.,* US Patent No. 7,246,360 (issued July 17, 2007); and
- **Fielder:** *Fielder,et al.,* US Patent No. 5,963,646 (issued October 5, 1999).

Overview of the Application

[0014] The Application describes determining and signaling if encryption uses weak keys or algorithms in order to avoid a "false security" by intercepting cryptographic API calls. For each such API the tool verifies the encryption parameters used and makes sure that the keys are secure enough.

Cited References

[0015] The Examiner cites Elgamal as the primary reference in the obviousness-based rejections. The Examiner cites De Bonet as a secondary reference and Fielder as a tertiary reference in the obviousness-based rejections.

[0016] Elgamal describes a method and apparatus for controlling the use of cryptography such that products utilizing these controls may be exported in accordance with United States export laws, and/or imported into other countries that place additional restrictions on the use of cryptography.

[0017] De Bonet describes a plug-in API for protocol and payload transformation.

[0018] Fielder describes a secure deterministic encryption key generator.

Lack of *Prima Facie* Case of Obviousness (MPEP § 2142)

[0019] Applicant disagrees with the Examiner's obviousness rejections of claims 1-7, 10-21, 23-33 and 35-40 under 35 U.S.C. § 103(a) as being unpatentable over Elgamal in view of DeBonet. Applicant respectfully traverses the rejection of these claims and asks the Examiner to withdraw the rejection of these claims. Arguments presented herein point to various aspects of the record to demonstrate that all of the criteria set forth for making a prima facie case have not been met.

Independent Claims 16 and 29

[0020] Applicant submits that Elgamal and DeBonet either alone or in combination do not disclose, teach, or suggest at least the following elements as recited in these claims (with emphasis added):

- "selectively perform[ing] at least one **correctness detection action based on said requested cryptography service**"

[0021] The conformance test of Elgamal, relied upon in the rejection, occurs *during implementation of a cryptographic function.* Specifically, in the reference, the function *is performed*, then the results are compared to a "known compliant implementation of the same algorithm," (c. 5, ll. 60-63). Notably, the selective performance of the claimed "correctness detection action [is] based on said requested cryptography service." In the claims, the cryptography service is **requested** not *implemented* as in the reference. Elgamal, disclosing a *perform and compare for conformance operation* fails to suggest the claimed "**correctness detection action based on said requested cryptography service**." DeBonet fails to remedy this deficiency.

[0022] As shown above, the combination of Elgamal and DeBonet does not teach or suggest all of the elements and features of these claims. Accordingly, Applicant asks the Examiner to withdraw the rejection of these claims.

Independent Claim 1

[0023] Applicant submits that in addition to the deficiency discussed above regarding independent claims 16 and 29, Elgamal and DeBonet either alone or in combination do not disclose, teach, or suggest at least the following elements as recited in this claim (as amended with emphasis added):

- "the selectively performing at least one correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold includes determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold, wherein determining if the cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold includes comparing a size of the cryptographic key with the at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length"

[0024] As discussed above, the conformance test of Elgamal, relied upon in the rejection, occurs *during implementation of a cryptographic function.* Specifically, in the reference, the function *is performed*, then the results are compared to a "known compliant implementation of the same algorithm," (c. 5, ll. 60-63). Furthermore, Elgamal does not disclose, teach, or suggest a "correctness detection action based on the requested cryptography service and the at least one cryptography service parameter threshold include[ing] determining if a cryptographic key associated with the requested cryptography service is suitable for use based on the at least one cryptography service parameter threshold ... include[ing] comparing a size of the cryptographic key with the

at least one cryptography service parameter threshold, wherein the size of the cryptographic key is identified by bit length," as recited in the claim. DeBonet and Fielder either alone or in combination with Elgamal fail to disclose teach or suggest each of the elements and features of this claim as amended.

[0025] As shown above, the cited references do not teach or suggest all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

Dependent Claims 2, 3, 6-10, 13-15, 17-28, and 30-43

[0026] These claims ultimately depend upon one of independent claims 1, 16, and 29. As discussed above, claims 1, 16, and 29 are allowable over the cited references. It is axiomatic that any dependent claim which depends from an allowable base claim is also allowable over the cited references. Additionally, some or all of these claims may also be allowable for additional independent reasons. Applicant respectfully requests that the Examiner withdraw the rejection of each dependent claim where its base claim is allowable.

Conclusion

[0027] All pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application. If any issues remain that prevent issuance of this application, the **Examiner is urged to contact me before issuing a subsequent Action**. Please call or email me at your convenience.

Respectfully Submitted,

Lee & Hayes, PLLC
Representatives for Applicant

/Bea Koempel-Thomas 58213/ Dated: 11/30/2008

Bea Koempel-Thomas (bea@leehayes.com; 509.944.4759)
Registration No. 58,213

Assistant: Cherri Simon (cherri@leehayes.com; 509.944.4776)

Customer No. **22801**

Telephone: (509) 324-9256
Facsimile: (509) 323-8979
www.leehayes.com